

# ABQ ThunderBird Cup v3.0 Alpha Workshop

Workshop Analysis 2016

Lee, Wellington | Morris, Tyler | Chu, Andrew

Sandia National Laboratories

Katrina Gilmore

Paine College

Joshua Russ

Voorhees College

Aliyah Carter

Norfolk State University



**THUNDERBIRD CUP**  
A CECOR Cyber Education Program



**Sandia  
National  
Laboratories**



**CECOR**  
Consortium  
Enabling  
Cybersecurity  
Opportunities &  
Research



**U.S. DEPARTMENT OF  
ENERGY**

## [Abstract](#)

The Albuquerque workshop was used to implement and test the newly designed ThunderBird Cup v3.0 (TBC3) system. The TBC3 system integrated a client side scoring system, interactive system elements and an online scoreboard to keep students grades 7-11 engaged.

## Table of Contents

ThunderBird Cup v3.0.....	2
Purpose Statement.....	2
Goals .....	2
Program Explanation .....	2
History.....	2
Participant Breakdown .....	2
Training Breakdown .....	3
Lesson Breakdown.....	3
Lesson Surveys .....	3
Storyline.....	4
Storyline Synopsis.....	4
Current Storyline State, Improvements, and Test Data.....	4
Future Goals and Progression .....	4
Client/Server Scoring System.....	5
Client Scoring .....	5
Client Action Scoring.....	5
Server Scoring.....	5
Virtual Machines .....	5
Thursday Educational Image Results .....	6
Friday Competition Image Results.....	7
Multiday Results.....	8
Virtual Machine Overview .....	8
Team Mentors.....	9
Katrina Gilmore   Paine College .....	9
Joshua Russ   Voorhees College.....	9
Aliyah Carter   Norfolk State University .....	10
Workshop Evaluation and Surveys.....	11
Surveys.....	11
Post Evaluation.....	13

## ThunderBird Cup v3.0

The ThunderBird Cup v3.0 (TBC3) program falls under the Minority Serving Institution Pipeline Program (MSIPP) that aims to establish a world-class workforce development, education and research program that combines the strengths of Historically Black Colleges and Universities (HBCUs) and national laboratories to create a K-20 pipeline of students to participate in cybersecurity and related fields.

### Purpose Statement

The ThunderBird Cup v3.0 (TBC3) system implements all previous v2.0 features with added improvements to design, efficiency, power, and interface. The ThunderBird Cup v3.0 system is designed to integrate an educational environment and game into one platform. This allows us to provide an interactive learning environment that promotes adaptive reasoning vs. routine, unmindful thinking.

### Goals

- Educate and engage students grades 6-12 in fields related to cybersecurity
- Provide cybersecurity focused exercises that engage students grades 6-12
- Provide the consortium with an education model for future TBC competitions
- Provide an integrated client/server scoring system to track students' progress

### Program Explanation

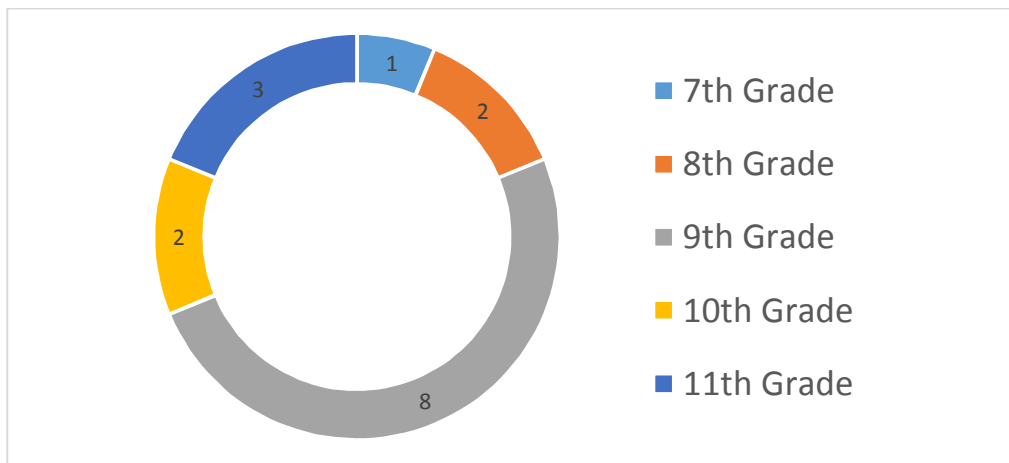
The ThunderBird Cup v3.0 system is a cybersecurity awareness exercise created by Sandia National Laboratories. The program uses hands on training and competition to engage students in the exciting field of cybersecurity in the hope of leading them to further their education in STEM related fields.

### History

The ThunderBird Cup program was first tested in 2014 at the University of the Virgin Islands (UVI). Students were given hands on experience in cybersecurity to help prepare them for the upcoming year of CyberPatriot. Since then, Sandia has implemented two more workshops at UVI that allow for testing of future ThunderBird cup systems and methods. Today, Sandia is beginning full development of the ThunderBird Cup v3.0 system.

### Participant Breakdown

A total of 16 students ranging from grades 7-11 attended the three-day workshop.



# Training Breakdown

## Lesson Breakdown

- Lesson 0 –Fundamentals
- Lesson 1 –Window Navigation
- Lesson 2 –Administrative Tools
- Lesson 3 –Malware Protection/Passwords
- Lesson 4 –Remote/File Sharing
- Lesson 5 –Programs/Task Scheduler

Each lesson included tutorial videos on the related subject along with “try it” exercise instructions to have students test their new skills on a training machine. Each student was placed in a predesigned team with a team mentor. Lessons one through five were self-guided and allowed teams to progress at a more comfortable pace. Team mentors provided explanations for exercises and answered questions during the training. At the end of each day teams competed against each other to test their new skills.

## Lesson Surveys

Each lesson has pre and post lesson surveys to gage student retention. During this exercise two training methods were used: self-guided instruction for lessons one and two and mentor lectures for lessons three through five. The survey results below express the percentage of correctly answered questions from six teams. Yellow shading represents no change, green- positive change, and red- negative change.

### Self-Guided

	Lesson 1			Lesson 2		
	Pre	Post	% -/+	Pre	Post	% -/+
Question 1	100%	100%	0%	67%	100%	33%
Question 2	100%	100%	0%	0%	17%	17%
Question 3	33%	67%	33%	50%	83%	33%
Question 4	N/A	N/A	N/A	83%	100%	17%

### Lecture

	Lesson 3			Lesson 4			Lesson 5		
	Pre	Post	% -/+	Pre	Post	% -/+	Pre	Post	% -/+
Question 1	67%	67%	0%	100%	83%	-17%	33%	33%	0%
Question 2	83%	100%	17%	33%	83%	50%	83%	83%	0%
Question 3	0%	67%	67%	100%	100%	0%	33%	17%	-17%
Question 4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

# Storyline

## Storyline Synopsis

The current storyline of TBC3 Alpha revolves around military drone manufacturer S-Drones, who has recently become the victim of a security breach. As the storyline progresses, it is revealed that Adam Davidson, CEO of competitor company DarkTech, has bribed an indebted employee (Devin Sinjin) to hack into S-Drones network in exchange for a monetary reward. While initially hesitant, Sinjin eventually performs this job, but gets caught. TBC teams are brought in at this stage of the story as security consultants, tasked to figure out the cause of the incident, the main actor, and his motive.

## Current Storyline State, Improvements, and Test Data

The storyline for TBC3 Alpha tests a new style of narrative that we plan to have implemented in the final rollout of the completed TBC3. In this Alpha test, the overall storyline moved away from the more fantastic interstellar plot seen in TBC2, and towards one more realistic to the current global cybersecurity status quo. In this sense, the overall storyline has become more streamlined and objective. Teams now have the ability to create their own identity to represent their role in the game, allowing for increased team capacity and maintained student interest in the competition. In addition, teams no longer search for small objects such as “artifacts” or “clues” but instead work to find forensics relating to the attacker and his background/identity. This is a completely new change, and one that we see as constructive and positive. Each team is now a “good guy” working to track down the “bad guy,” and spends less time piecing the many small details together (as seen in TBC2,) in exchange for larger more comprehensive segments. The latter benefit of the new storyline proved extremely effective in our run-through, as students no longer were confused by the disproportionate amount of bits that needed to be tied together in order to achieve a solid understanding of the story, and instead were able to construct fairly accurate narratives of the situation. A sample forensics narrative response is as follows:

“Derrick is a information Security Engineer at DarkTech. After Derrick's financial company, Epiphany Financial Services, emailed him to his fake alias (Max Dekker) about the money he owes them, Derrick searched for ways to get money to pay the company. The next day he went to work and his situation was overheard by staff members, including Adam Davidson, the CEO of DarkTech. Adam sent a message to Derrick and his job was to hack the S-Drone system. At first he was unsure until Adam mentioned that his profit would help him repay his financial company. Derrick took the job and was at first successful. He eventually was found by a staff member of S-Drones.”

As seen in this example, the new storyline method used in TBC3 Alpha integrates itself much more deeply into the overall TBC system, and produces flushed out, complete plot summaries that are objective and very close to the actual planned scenario.

## Future Goals and Progression

The new storyline approach resulted in an overall improvement to the TBC system, and will be further revised for added integration, depth, and general quality for the official TBC3 rollout.

## Client/Server Scoring System

The TBC3 scoring system is a Sandia developed system that gathers preconfigured flags from connected clients and reports to the scoring server that allows for full analysis of team results. The client side system works in the background without the user's knowledge. The server side system allows teams to actively monitor what tasks they have completed and their overall score. Teams are also able to see other team's overall scores. Administrators are given special access to view what tasks each team has completed along with the power to reset point values and manage server data.

### Client Scoring

The alpha test of the TBC3 scoring system worked remarkably well at collecting and sending data to the server. When compared to TBC2, TBC3 increased functionality and reduced overall system usage by approximately five percent. Students were not able to get into the scoring client and don't have access to its source code or processes. The team login issue was somewhat resolved by adding a verification line and using only numeric values for team ids. However, team login prompts would sometimes execute slowly after the image was started. We are currently working on a solution for this problems and will have a full fix before full distribution of TBC3. Other than these issues, the scoring system worked as expected with no significant failures.

### Client Action Scoring

The newly designed TBC3 action script allows for the scoring system to interact with users. The system is designed to create popup windows, shutdown, lockout, logoff the system and create many other system related issues during the competition. The purpose of this system to keep students engaged and actively participating to prevent these attacks. The new script functioned as expected, but needs improvements to timing and efficiency. These improvements will be made before full distribution of TBC3.

### Server Scoring

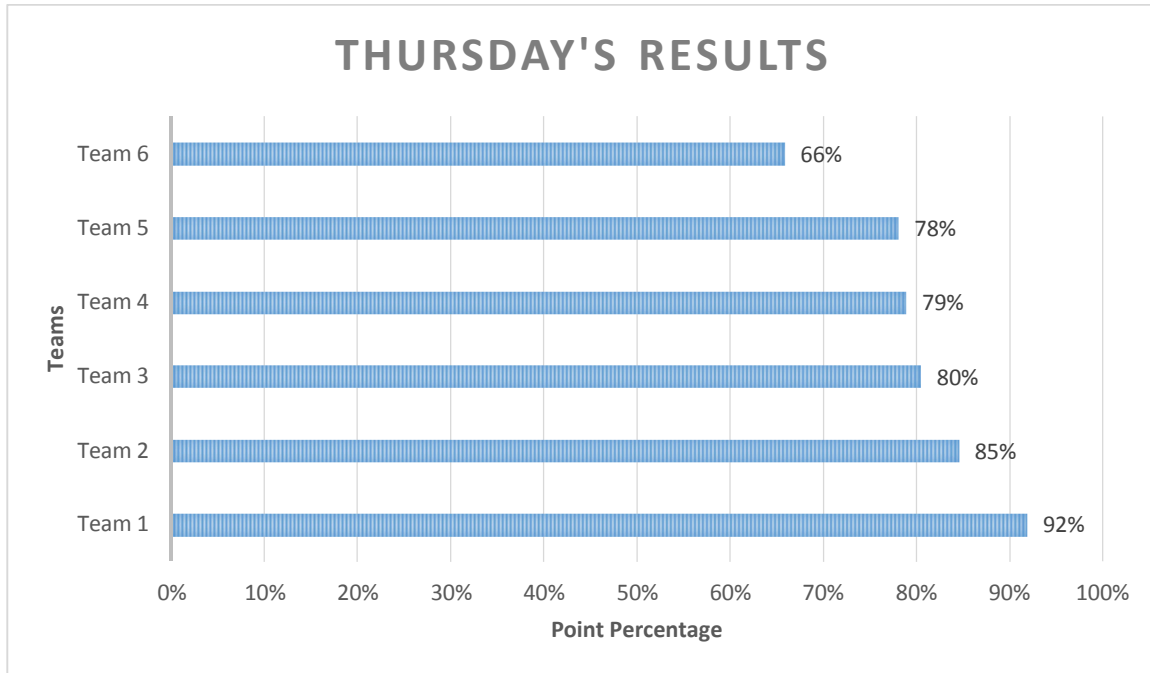
The Thunderbird Cup Server worked well during the event. In terms of functionality, the server correctly reported completed tasks to each team and showed their points correctly on their user interface. Based on the information sent from the PowerShell scripts on the clients, the server correctly logged and kept track of each team's progress. However, we did encounter issues with overall point values and keeping track of points for multiple images. Despite these setbacks, the implementation of the new scoring system with account registration and an improved user interface went well and the server ran throughout the duration of the event.

## Virtual Machines

A virtual machine is defined as one instance of an operating system along with one or more applications running in an isolated partition within the computer. It enables different operating system to run in the same computer at the same time. It is like running Windows 7 inside of Windows 7. We utilize virtual environments to allow for an easy roll out of our scoring system, have images that are preconfigured, and to have an environment that students can damage without impacting the actual computer.

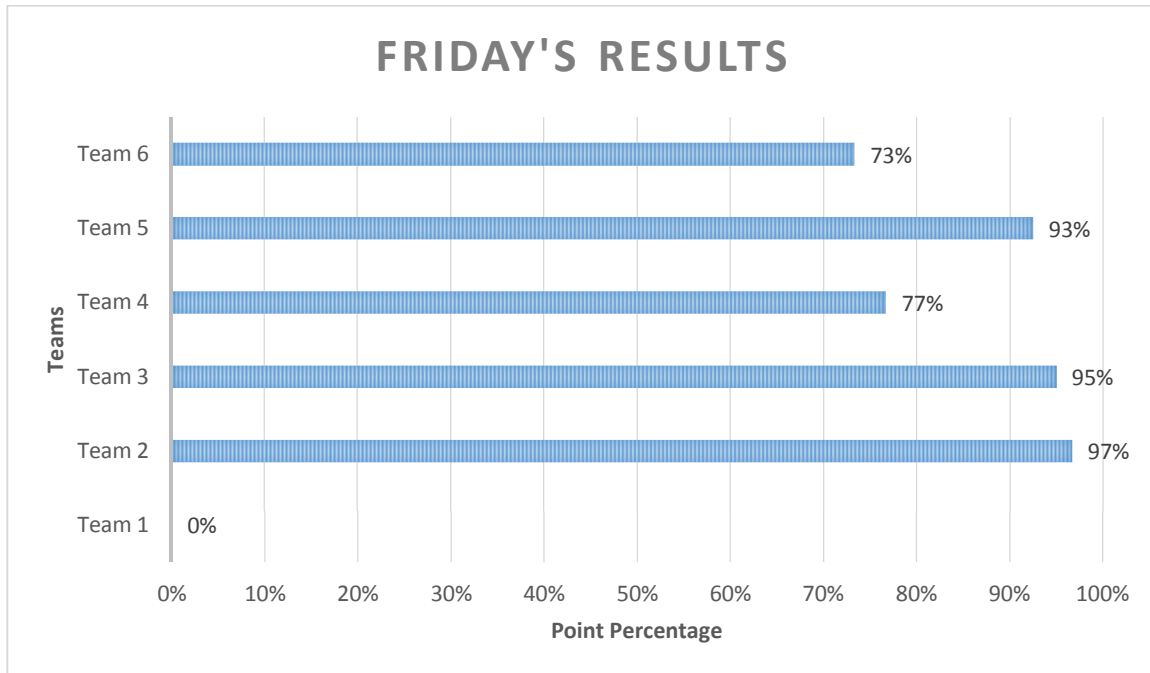
## Thursday Educational Image Results

The data below was compiled by our ThunderBird Cup ALPHA v3.0 scoring system at the end of Thursday's educational image. Once the self-guided educational lessons are finished, teams start the educational image. This Windows 2008 server image had a maximum of 123 points and teams actively competed for approximately two hours. All scores have been converted to percentages for readability.



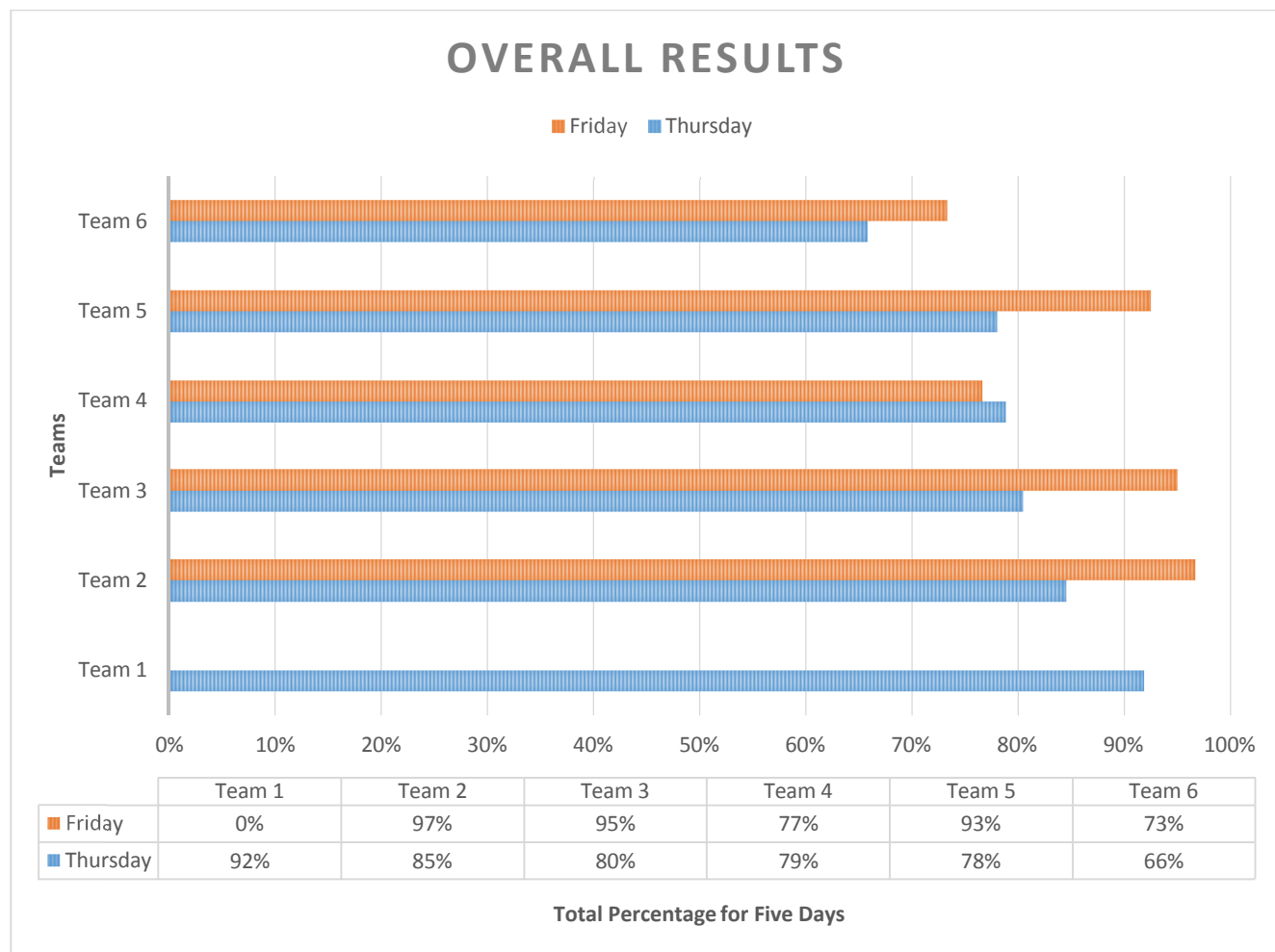
### Friday Competition Image Results

The data below was compiled by our ThunderBird Cup ALPHA v3.0 scoring system at the end of Friday's competition image. Teams are not given any educational lessons on this day and are presented with just the competition image. This image is the most difficult image out of all the days and is designed to truly test their educational retention. This image introduced our newest element, dynamic interaction, which allows the system to react to changes made during the competition and interact with the user. This Windows 7 image had a maximum of 120 points and teams actively competed for approximately two and half hours. All scores have been converted to percentages for readability. Team one was consolidated into team three because of an absence. Per that, team one has no data.



## Multiday Results

The data below is a multiple day outlook for all six teams. This data has an x-axis with the total number of 243 point from all five days. All scores have been converted to percentages for readability. Team one was consolidated into team three because of an absence. Per that, team one has no data on Friday.



## Virtual Machine Overview

Virtual environment testing allows us to gather quantitative data on how students are learning during the three-day session. The virtual environments used during the three-day ABQ workshop were designed to be very challenging for students. The Friday image was especially difficult in order to gage the overall retention of the students. The data clearly indicates a major spike in scores as the days progressed and as the images became more challenging.

## Team Mentors

Mentors were assigned to each of the six teams participating. These mentors helped students with self-guided lessons, connecting images, and overall questions. Each of the mentors are visiting interns from the CECOR program.

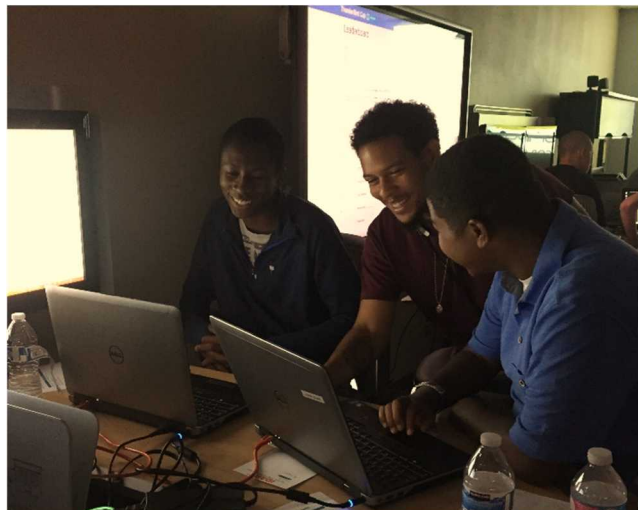
### Katrina Gilmore | Paine College

The high-level competitive environment allowed the students to learn about cybersecurity using hands-on skills to drive the program. It took the students a while to be able to find all the tools for the software on their own, but after going through the exercises a couple of times, they finally got the hang of it. They were not only able to navigate through the software independently, but they were able to mentor to other groups as well. If I could audit anything about the program, I would edit some of the learning software or have the students follow along with the video for understanding.



### Joshua Russ | Voorhees College

The fast paced environment of the ThunderBird Cup pushes students to learn basic cybersecurity tips competitively amongst their peers. I thought we created a great atmosphere for them to absorb as much knowledge as possible in a 3-day period. Students seemed to enjoy the competitive nature of the workshop. Even though the student's ages were a bit scattered, I could tell they were having a great time. The teams were also somewhat unbalanced in terms of skill; however, this can be hard to gauge with the small amount of time we had with them. Overall this program was well executed and I feel we enticed most of the kids to stay pursuant of their cybersecurity interests.



## Aliyah Carter | Norfolk State University

Overall the program was very educational and successful. The ThunderBird Cup provided many aspects of basic computer security that helps students not only practice but to learn for real world application. TBC helped the students understand the basic vulnerabilities in the computer's security, and how they can fix it. From a mentor stand point, I feel though the students of various ages were able to understand and complete the task given to them. They were diligent and focused on the training as well as the competition. The scoreboard itself added excitement to the game, as the students raced to finish the training and competitions to have the highest points. The competitions were hands on, and allowed students to apply the knowledge they learned. The students were interested and excited about the new things they were learning. There are a few things that should be improved, while being in one room, the training videos were very loud and distracting, but a way to fix this could be providing each group with a particular space so they can focus and hear. The students should be provided with notepads, and pens so they can take notes on the things they have learned. Also, some of the videos were out of order and for the next competition should be reordered. The TBC was very successful, and I feel as though the students left with more knowledge than they came in with. I am grateful to be a part of such a program and I hope to be able to participate again!

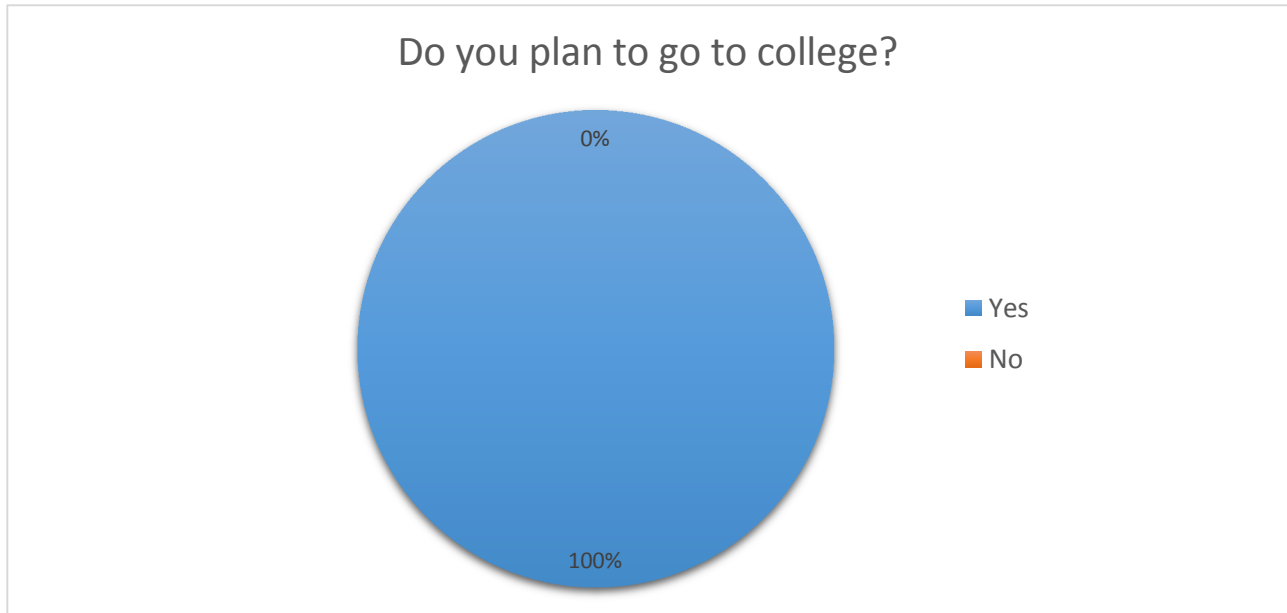


## Workshop Evaluation and Surveys

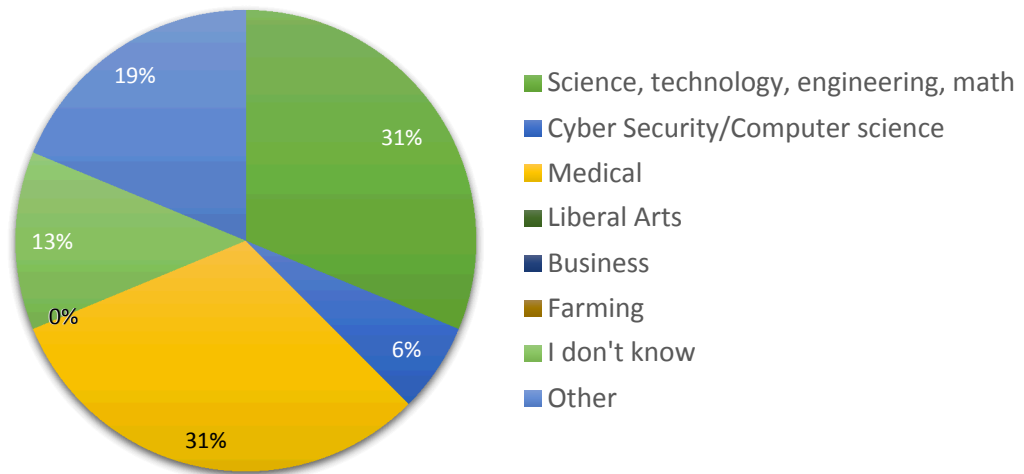
The ThunderBird Cup program strives to become better each time it is implemented. With that in mind, each workshop has surveys and an end of course evaluation to help improve the overall program. The data collected has been compiled below.

### Surveys

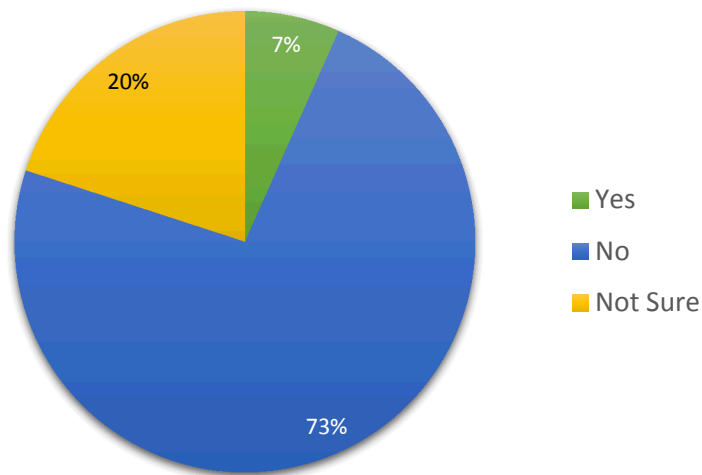
Students were asked quick questions during the check-in process to help gauge interest and knowledge level.



### What degree area are you looking into?

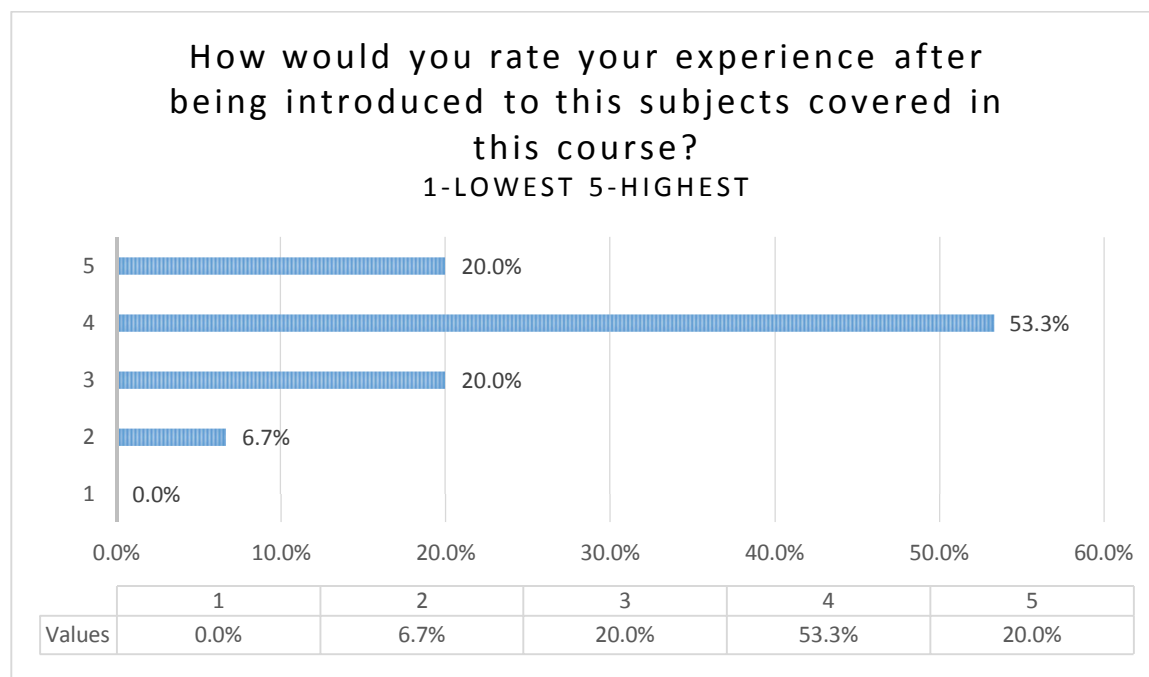
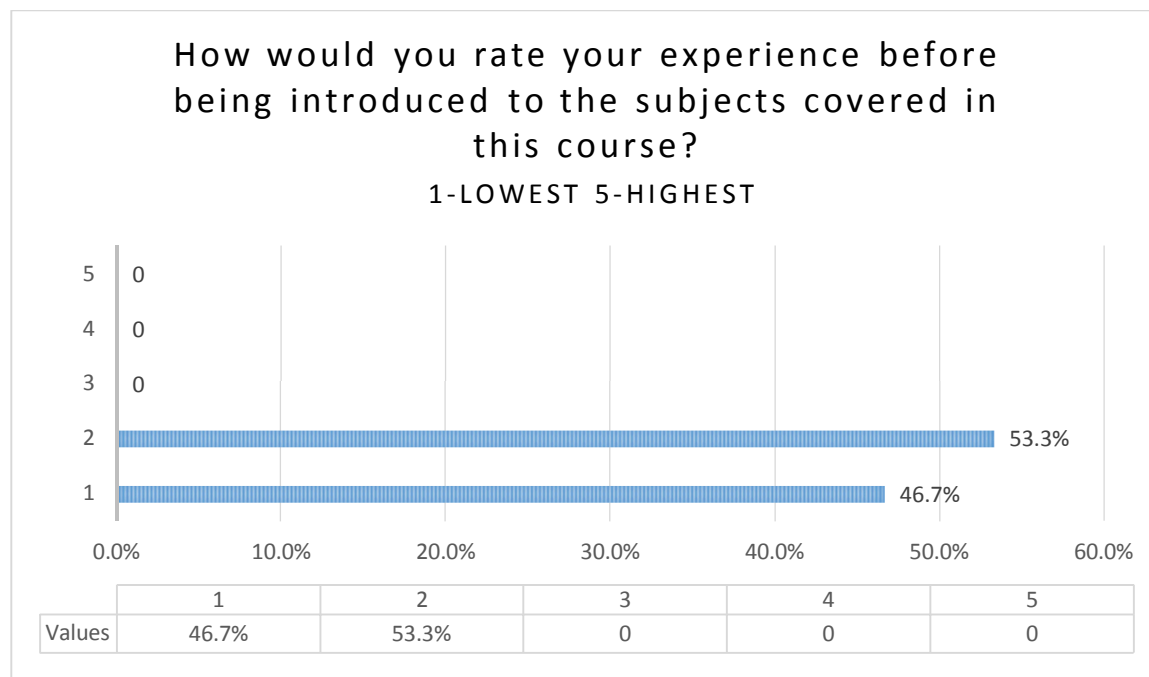


### Have you learned about cyber security in school?

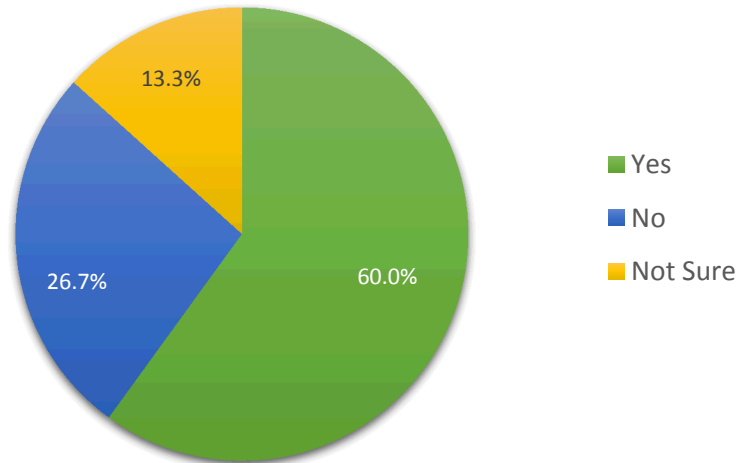


## Post Evaluation

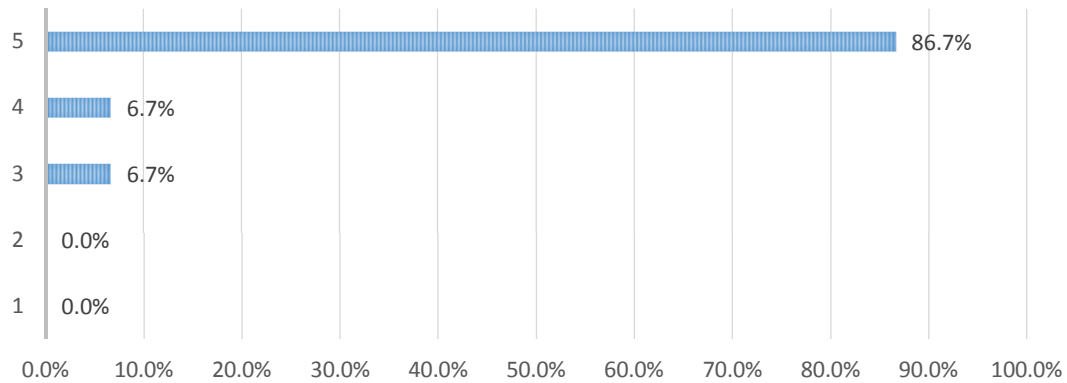
Post evaluations were conducted on the last day and were voluntary to participate in. The compiled results are below in random order.



After this course are you more likely to pursue a degree in science, technology, engineering, math, and or cyber-security/computer science



How helpful was your mentor during the learning process?  
1-LOWEST 5-HIGHEST



	1	2	3	4	5
Values	0.0%	0.0%	6.7%	6.7%	86.7%

### What did you like most about this course?

Having my mentors help me out as much as they could before we actually went into the actual competition.
Learning about more settings on the computer. It was interesting learning about the Administrator Tools.
The Interactive images
Being able to interact with the computer and learning from the mistakes.
Playing with all the VM images
All of the computer work
Working in a group and with a dedicated mentor.
Getting to know how to get around on a computer.
I liked the tutorials. They really helped.
free food and learning about hacking and more in depth computer settings
I liked the competitions
It was very interesting and it showed me a possibility for a good career.
It was very interesting and it showed me a possibility for a good career.
all the competition
WORKING TOGETHER AS A TEAM

### What did you like least about this course?

What I didn't like as much as the others would have to be doing the surveys but now being in the actual competition I think they have helped a lot.
It was not quite as I expected. I thought that we would be creating firewalls and such instead of working with settings that you could change on any computer.
N/A
There wasn't much I disliked about the course.
Cooperation
Nothing
not having enough breaks
large groups even though there are only three people always one person is left out usually.
I think that some of the information was not explained well enough.
running only one VM
Nothing
The Forensics File was extremely picky.
The Forensics File was extremely picky.
the videos were hard to understand
IT WAS SOMEWHAT CONFUSING

### **If you could change this course, what would you change?**

What I would change in this course is really nothing.

I would make it more like I expected.

I would add more Images

Maybe a faster program so we wouldn't have to wait for the scoreboard to update.

Having more teams to compete against

nothing

have two people in a group

smaller groups and more computers to use to get the job done.

I would add more tutorials

run multiple VM's, more breaks

Nothing

Nothing.

Nothing.

make the videos slower and easier to understand

NOTHING

### **Please place any additional comments below:**

Shout out to Katrina and James for all the help that you have given the Dark Assassins. It really made this experience so much fun and makes me want to come back. You guys are the best.

I enjoyed the course, however I wish we could see the stuff that was not just on the surface of the computer. I was expecting to be able to see how it was programmed and things like that.

Loved the course

nothing

Thank you for putting this program together and putting your time and effort into this!!!

All the staff in helpful and ready to assist.

great course overall!

THE COMPATISHON WAS AWSOME!!!